UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE MATEMÁTICA

Introdução à Criptografia de Chave Pública

Elisangela Rodrigues Santos
01/julho/2005

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE MATEMÁTICA

Introdução a Criptografia de Chave Pública

Trabalho de Conclusão de Curso
em Matemática – Habilitação
Licenciatura, do Departamento de
Ciências Físicas e Matemáticas
da Universidade Federal de Santa Catarina,
Orientada por Licio Hernanes Bezerra.

Elisangela Rodrigues Santos
01/julho/2005

A meus pais,
Aliria e Silvano
pela confiança que em mim
foi depositada.

Agradecimento

A meus pais, Aliria e Silvano que,
me proporcionaram a oportunidade de sempre aprender;
A meu namorado, Tiago Z. Beretta, pelo carinho e compreenção,
Ao professor Licio Hernanes Bezerra que,
me ajudou nos momentos difíceis,
À banca examinadora, professores Carmem S. C. Gimenez
e Milton dos S. Braitt, por aceitarem avaliar este trabalho,
Ao professor Milton, pela colaboração na exposição
deste trabalho; Aos amigos da secretaria, Silvia, Iara e Alcino.

Resumo

Neste trabalho será introduzido o método criptográfico RSA, baseado na escolha de dois números primos muito grandes. Para que possamos determinar estes números, discutiremos alguns conceitos de aritmética modular e testes de primalidade.

Sumário

Introdução

A palavra criptografia tem a seguinte origem: kriptós = escondido, oculto e grápho = grafia. Ou seja, criptografia é a arte ou ciência de escrever em cifras ou em códigos, de tal maneira que somente o destinatário tenha permissão para decifrar ou compreender a mensagem, pois a criptografia converte textos originais em uma informação transformada, que chamamos de texto cifrado. Sendo mais rigoroso, Criptografia é o estudo dos métodos para cifrar ou codificar uma mensagem, de tal forma que só o destinatário legítimo seja capaz de interpretar o conteudo da mensagem. Outros termos utilizados são:

- Criptoanálise (kriptós = escondido, oculto e análysis = decomposição) – é o estudo de métodos para decifrar uma mensagem codificada sem ser o destinatário legítimo.
- Criptologia (kriptós = escondido, oculto e logo = estudo, ciência) – é a junção de Criptografia e da Criptoanálise.

Normamente usamos as palavras **decodificar** e **decifrar** com o mesmo sentido. Não nos damos conta que, ao decodificarmos uma mensagem, estaremos realizando o processo que um usuário legítimo do código faz quando recebe uma mensagem codificada. Por outro lado, ao decifrarmos, estaremos realizando o processo de ler a mensagem mesmo não sendo o usuário do código.

Desta forma, o principal propósito da criptografia é permitir que seja feita com segurança a transmissão da mensagem de forma restrita ao usuário.

Nos tempos atuais, a criptografia está fundamentada em algoritmos complexos, usados para cifrar mensagens, que são usadas nas comunicações militares, diplomáticas e transações comerciais, garantindo assim *sigilo, integridade, autenticação do usuário, autenticação de remetente, autenticação do destinatário e de atualidade.* Esta segurança depende de técnicas matemáticas para que sejam feitas a codificação e decodificação de uma mensagem, de tal forma que este código seja difícil de ser decifrado, principalmente através de computadores.

O primeiro código de chave pública foi desenvolvido por L. R. Rivest, A. Shamir e L. Adleman – RSA. O código funciona com duas chaves: uma que codifica (chave pública); e outra, que decodifica. A segurança está em como gerar e distribuir as chaves. O RSA é considerado atualmente um dos mais seguros métodos de criptografia, pois ao se tentar decifrar uma mensagem criptografada na RSA depara-se com uma dificuldade muito grande.

Este trabalho abordará história e conceitos matemáticos da criptografia. No Capítulo 1, trataremos da História da Criptografia e das diferenças entre Criptografia Clássica e a RSA. No Capítulo 2, será exposto o método de codificação e decodificação **RSA**, conceitos de aritimética modular, divisão nos inteiros, segurança e assinaturas do RSA. No Capítulo 3, serão abordados testes para determinar quando um número é primo. No Capítulo 4, apresentaremos uma aplicação do método RSA.

Capítulo 1

A Criptografia

1.1 História da Criptografia

Faremos um passseio por diversos momentos da história, em que a criptografia esteve presente na mente humana, especialmente na esfera do poder.

Começamos na Antiguidade, quando a criptografia não era ligada a sistemas de códigos e cálculos matemáticos, era apenas resultado de idéias criativas, iniciando assim a base para a criptografia.

O primeiro exemplo documentado da escrita cifrada foi numa vila egípcia perto do rio Nilo, chamada Menet Khufu. Um arquiteto do faraó Amenemhet II construiu alguns monumentos para o faraó, os quais foram documentados em tabletes de argila, e, é claro, não poderiam cair em mãos públicas. O escriba teve então a idéia de substituir algumas palavras ou trechos do texto por símbolos, de tal forma que, se o documento fosse roubado, o ladrão não encontraria o caminho que o levaria a um suposto tesouro.

Percorrendo pela Antiguidade, por volta de 1500a.C, o Egito, China, Índia e Mesopotâmia desenvolveram a **Esteganografia**, que se destacou através dos seguintes métodos.

- Tatuagens com mensagens na cabeça de escravos

- Marcas em madeiras de placas de cera, que eram depois cobertas com cera nova
- Mensagens dentro do estômago de animais de caça e também de humanos

Por volta de 600 a 500 a.C, os escribas hebreus escreveram o livro de Jeremias, usando como cifra a substituição simples pelo alfabeto reverso, conhecido como **Atbash**. As cifras da época eram as seguintes: **Atabash, Albam e Atbah**, que eram conhecidas como Cifras Hebraicas.

No século IV a.C, houve a invenção de um sistema de comunicação ótico, parecido com o telégrafo, o conhecido **relógio de água**, inventado por Enéas, o Tático. Logo, em seguida, o general Tucídides usa o método conhecido como **Bastão de Licurgo**, sendo este talvez o sistema criptográfico mais antigo.

Por volta de 300 a.C, é atribuido a Políbio, um historiador grego, uma cifra de substituição que converte os caracteres da mensagem em números, o chamado **Código de Políbio**. Perto de 50 a.C, Julio Cesar usa sua cifra de substituição para cifrar mensagens governamentais, que eram compostas pela alternância de letras, desviando–as em três posições. O **Código de César** é o único da antiguidade usado ainda hoje, e todas as cifras baseadas na substituição cíclica são conhecidas como Código de César.

Na Idade Média, há certo dominio da escrita e da matemática, e o homem passa a se especializar em criptografia. Nesta época, os sistemas se tornam mais sofisticados, com estudos cada vez mais avançados na Criptoanálise. Esta época na Europa foi conhecida como período das trevas e a criptografia não escapou de perseguições. Desta forma, muito sobre o assunto foi perdido, pois a criptografia era considerada magia negra ou bruxaria.

De 700 ao início do século XI, muitos Árabes escreveram obras sobre criptografia, principalmente métodos para decifrar sistemas. Em 1187, Ibn

Dunainir em seu livro **Explicações claras para a solução de mensagens secretas** expõe um sistema inovador: cifras algébricas, ou seja, a substituição de letras por números, de tal forma que a transformação da mensagem original em cifra seja feita aritmeticamente. Por volta de 1200, o frade inglês Roger Bacon descreve sete métodos de cifras. A contribuição arabe-islâmica foi significativa com a invenção da criptoanálise. A denominação **'Cifra'** vem da palavra árabe 'sifr', que significa 'nulo'. Em Veneza, por volta de 1300, foi criada uma organização especializada com o objetivo de manipular a criptografia. Em 1378, o antipapa Clemente VII decide unificar as cifras da Itália e designou a tarefa a Gabriele Lavinde, que compilou um manual contendo uma coleção de cifras manuais, do qual o Vaticano tem uma cópia de 1379. Este manual, que une cifras e códigos, foi usado por aproximadamente 450 anos. Entre 1400 e 1500, foram editados sistemas homofônicos e polialfabéticos, sendo que neste último sistema usava–se um **Disco de Cifragem**. Esta cifra foi quebrada por volta de 1800.

Já na Idade Moderna, houve uma explosão no estudo da criptografia, com troca de idéias, experiências e a publicação de trabalhos. Em 1518, Johannes Trithemius escreveu o primeiro livro impresso sobre criptografia. Após 32 anos, foi publicado por Girolamo Cardano o primeiro procedimento com auto-chave, porém seu sistema era imperfeito. O nome dado a este sistema era **Grelha de Cardano**. No final do século XVI, a França começa a consolidar sua liderança na criptoanálise, com Sir Francis Bacon, o inventor de um sistema esteganográfico, denominando seu alfabeto de **Biliteral**, pois utilizava a combinação de duas letras A e B em grupos de cinco. Esta cifra foi conhecida como **Cifra de Bacon**; hoje, é classificada como codificação binária de 5 bits. Em 1663, Athanasius Kirchner, estudioso e matemático alemão, transformou as cifras multialfabéticas em cifras numéricas. Leibniz inventou, 7 anos depois, a máquina de calcular usando uma escala binária que, reformulada, é utilizada até hoje e é conhecida como **Código ASCII**.

Em 1691, Antoine Rossignol elaborou a Grande Cifra de Luís XIV. Esta cifra era muito sofisticada. No entanto, foi quebrada ao redor de 1890. O século XVIII é a época da espionagem das Câmaras Escuras na Europa. Neste momento, em Viena, foi constituida uma das mais eficientes equipes, que decifravam cerca de 100 cartas diariamente.

No século XIX, a comunicação passou da oral e escrita para o uso do telégrafo, tambores e sinais de fumaça. Estes métodos não são criptográficos, porém exigem codificação e decodificação, o que indica que Linguagem, Comunicação e Criptografia estão ligadas pela história. Desta forma, entre 1790 e 1900 a criptografia se dissemina no ocidente, começando assim a surgir máquinas e dispositivos sofisticados, um grande avanço na criptografia mecanizada, juntamente com os primeiros sistemas de comunicação a distância. No início de 1800, o Coronel Decius Wadsworth produziu um disco cifrante, contendo engrenagens, com números diferentes de letras **no alfabeto original e cifrante**, o que resulta numa cifra progressiva na qual os alfabetos são usados irregularmente. O Código Braille é criado em 1834 e é contituido por 63 caracteres, cada um composto de 1 a 6 pontos, dispostos em uma matriz ou célula de seis posições. Este sistema é reconhecido internacionalmete e utilizado até hoje. Em 1840, Samuel Morse desenvolve o código que recebeu seu nome, sendo na verdade um alfabeto cifrado em sons curtos e longos. Charles Babbage, hoje conhecido como O **Pai do Computador**, projeta a primeira máquina de cálculo sofisticada, conhecida como *Máquina das Diferenças*. Na mesma época, surge com Charles Wheatstone a *Cifra Playfair*, que era composta por uma matriz de letras com chaves para produzir cifras digráficas, facilmente usadas no campo de batalha. Em 1893, ocorrem as primeiras transmissões de sinais telegráficos e de voz humana por telefonia sem fio, em São Paulo, Brasil, pelo padre Roberto Landell de Moura, porém o mérito de inventor fica com o italiano Marconi.

O século XX foi marcado por duas guerras mundiais, e avanços na ciência

e tecnologia. O aumento da informação nos possibilitou a chegada da era digital, tomando conta assim de todos nós. Desta forma, no início de 1900, inicia–se com Guglielmo Marconi a era da comunicação sem fio, aumentando assim o desafio da criptografia. Em 1913, o capitão Parket Hitt reinventou o *Cilindro Cifrante*, abrindo caminho para o M–138 da Primeira Guerra Mundial. Após 6 anos, na Holanda, é criada uma máquina cifrante baseada em rotores, conhecida também como *Máquina Enigma* que, em 1923, é vendida aos alemães. Entre 1925 e 1933, o uso da criptografia não se limitava somente à alta sociedade, mas contrabandistas usavam a criptografia para seus feitos. De 1933 a 1945, a Máquina Enigma foi aperfeiçoada, transformando–se na ferramenta criptográfica mais importante da Alemanha nazista. Em 1960, o Dr. Horst Feistel desenvolve a cifra **Lucifer**, sendo que, anos depois, esta cifra serve de base para o desenvolvimento do *DES* e outros sistemas cifrantes. Em 1969, surge com James Ellis um sistema com chaves públicas e chaves privadas separadas. Oito anos depois, **Ronald L. Rivest, Adi Shamir e Leonard M. Adleman** começam a discutir como criar um sistema de chave mais prático, porém seguro, e em um ano o **Algoritmo RSA** é publicado. Em 1986, surge a criptografia com *curva Elíptica* sugerida por Miller, e, na década de 90, trabalhos com computadores quânticos e criptografia quântica começam a surgir. Em 1998, o código *DES* é quebrado em 56 horas; e em 1999, em apenas 22 horas e 15 minutos.

1.2 Criptografia Clássica x RSA

Desde a Antiguidade, tratando–se de mensagens secretas, o homem faz uso de artefatos e máquinas. No decorrer destes 2500 anos, houve diversos sistemas de cifragem, sendo que durante 1500 anos a criptografia não envolvia cálculos matemáticos em seu processo de cifragem. Os sistemas criptográficos nesta época tinham como unidade o caracter. As conversões se davam através de

duas operações básicas: a substituição e a transposição.

As cifras de substituição baseiam-se na substituição de um caracter por outro. Vejamos, como exemplo, a cifra de César, que substitui cada caracter por outro, três posições a seguir, em um alfabéto de 26 letras. Por exemplo:

- Frase original: A ARTE DA CRIPTOGRAFIA
- Frase Cifrada: D DVXH GD FULSXJUDILD

O comando ROT13 do sistema Unix é uma cifra de substituição, em que cada letra é rodada 13 posições.

Nas cifras de Transposição os carateres da mensagem se mantêm, porém sua ordem é trocada. Por exemplo:

- Frase original: A ARTE DA CRIPTOGRAFIA
- Frase Cifrada: RATAEA CDIPROG RTIAAF

Este tipo de criptografia se classifica como **Criptografia de Chave Simétrica**, ou seja, que utiliza a mesma chave para codificar e decodificar. Estes sitemas são conhecidos como *Criptografia Clássica*.

Atualmente, com algoritmos de criptografia próprios para o uso dos computadores, a unidade de manipulação neste momento são os bits, mantendo–se as duas operações anteriores, sendo elas a substituição e transposição. Na Criptografia RSA temos a chamada **Criptografia de Chave Assimétrica**, que utiliza uma **chave pública** e uma **chave privada** . A chave pública é usada para codificar e a chave privada para decodificar. O nome chave pública vem do fato de que você pode distribuir essa chave para qualquer pessoa, o que, por outro lado, não acontece com a chave privada. Para decodificarmos uma mensagem não precisamos da chave pública, porém a decodificação é inviável devido ao tempo que esta operação demoraria.

Portanto, entre a Criptografia Clássica e o Sistema RSA, a diferença está justamente no processo de codificação e decodificação, que poderemos entender melhor com a exposição feita no próximo capítulo do método RSA.

Capítulo 2

Criptografia RSA

A criptografia de chave pública ou assimétrica utiliza duas chaves que são relacionadas por uma função matemática. O que uma chave codifica a outra decodifica. Para que isto ocorra, o algoritmo que codifica e o algoritmo que decodifica deverão atender a três requisitos: Se C(M) é a mensagem codificada e D(C(M)) a mensagem decodificada, então:

1. D(C(M))=M, em que M seria a mensagem original.

2. Não pode ser simples a dedução de D, a partir de C.

3. C não pode ser decifrado através do ataque ao texto codificado.

O RSA satisfaz os três requisitos. Veremos como ele funciona e alguns conceitos matemáticos necessários para explicá-lo.

2.1 Pré–codificação

Esta é a primeira etapa do método RSA, em que convertemos a mensagem desejada em um número. Neste caso, iremos presumir que a mensagem a ser convertida tenha somente letras. Assim, observe a seguinte tabela:

$A \to 10$ $B \to 11$ $C \to 12$ $D \to 13$ $E \to 14$ $F \to 15$ $G \to 16$
$H \to 17$ $I \to 18$ $J \to 19$ $K \to 20$ $L \to 21$ $M \to 22$ $N \to 23$
$O \to 24$ $P \to 25$ $Q \to 26$ $R \to 27$ $S \to 28$ $T \to 29$ $U \to 30$
$V \to 31$ $W \to 32$ $X \to 33$ $Y \to 34$ $Z \to 35$

Quando enviamos uma mensagem, o correto é converter todo tipo de caracter: letras, números, pontuações, etc. Os valores associados a estes caracteres são escolhidos a seu gosto, desde que o receptor da mensagem também o saiba. Feita a associação, façamos a conversão da mensagem.

Exemplo:

Elisangela
1421128102316142110

Feita a conversão dos caracteres da mensagem, pelos valores associados, iremos passar a escolha de parâmetros.

Sejam **p** e **q** primos distintos. O par (p,q) são chamados de **parâmetros**, que formarão um terceiro número, **n**, de tal forma que n seja o produto de p por q, ou seja, $n = p.q$.

A última etapa da Pré-codificação é quebrar em blocos o número produzido pela conversão da mensagem que queremos enviar. Estes blocos devem ser menores que **n**.

Escolheremos números primos pequenos, para que possamos ilustrar as propriedades matemáticas da teoria dos números. Então sejam $p = 17$ e $q = 11$, a partir dos quais obtemos $n = 187$. Portanto, obtêm-se os seguintes blocos:

142 – 1– 182 – 8 – 102 – 31 – 61 – 42 – 110

Ao dividir os blocos devemos evitar o início de um bloco com **0** (zero). É bom evitar, também, blocos que sejam iguais a valores numéricos atribuidos a caracteres, pois assim dificultaremos a decodificação por contagem de frequência, que será, neste caso, essencialmente impossível.

2.2 Codificação e Decodificação

Terminada a fase da Pré–codificação, podemos passar a etapa de **codificação** da RSA propriamente dita. Para codificar uma mensagem, precisamos do inteiro positivo **n**, que é o produto dos primos escolhidos anteriormente, e de um inteiro σ que seja inversível módulo $\Phi(n)$, ou seja, temois que ter o mdc(σ,$\Phi(n)$) = 1. Mas o que seria $\Phi(n)$?

Definição 2.1 (Função de Euler): *Para cada número natural n definimos $\phi(n)$, a função de Euler, como sendo o número de inteiros positivos que não excedem n e são relativamente primos com n.*

Note que se conhecemos **p** e **q** é fácil calcular $\Phi(n)$, já que $\Phi(n) = (p-1)(q-1)$. Chamamos o par (n,σ) de **Chave de Codificação**.

Na Pré–codificação obtemos uma sequência de números ou blocos. Nesta etapa devemos codificar cada bloco separadamente, e a sequência de blocos codificados formará a mensagem codificada.

Como faremos para codificar um bloco b_k, com $k \in Z_+^*$, sabendo que b_k é um inteiro positivo e menor que **n**? Denotaremos por $C(b_k)$ o bloco codificado, que é definido como:

$$(b_k)^\sigma \equiv C(b_k) mod\, n$$

A fim de que possamos entender melhor o processo de codificação, será necessário que saibamos um pouco da `Aritmética Modular`. Inicialmente, vamos citar alguns conceitos.

2.2.1 Congruência

Definição 2.2 *Seja $n \in \mathbb{Z}$, em que $n > 1$. Sejam $a, b \in \mathbb{Z}$. Dizemos que a e b são* **congruentes módulo n** *se o resto da divisão de b por n é igual ao resto da divisão de a por n. Usaremos a seguinte notação para indicarmos que a e b são* **congruentes módulo n***:*

$$a \equiv b \bmod n$$

Exemplo 2.1 *Temos que $25 \equiv 13 \bmod 4$, pois o $resto(25, 4) = 1$ e o $resto(13, 4) = 1$.*

Existe outra forma para verificarmos a existência de uma congruência, e para isso usaremos a seguinte proposição.

Proposição 2.1 *Para quaisquer inteiros a e b, temos $a \equiv b \bmod n$ se, e somente se $n \mid (a - b)$.*

Demonstração:

$\Rightarrow$ *Como $a \equiv b \bmod n$, temos que $res(a, n) = res(b, n)$. Desta forma existem q_1 e q_2 tais que $a = q_1 n + r$ e $b = q_2 n + r$. Assim $a - b = n(q_1 - q_2)$, e então $n \mid (a - b)$.*

$\Leftarrow$ *Suponha que $n \mid (a - b)$ e que $r_1 = res(a, n)$ e $r_2 = res(b, n)$. Desta forma $a = nq_1 + r_1$ e $b = nq_2 + r_2$, em que $0 \leq r_1, r_2 \leq n$.*

Assim, $a - b = n(q_1 - q_2) + (r_1 - r_2)$. Como $n \mid (a - b)$ e $n \mid (n(q_1 + q_2))$ temos $n \mid (r_1 - r_2)$. Assim, $n \mid (|r_1 - r_2|)$ e $|r_1 - r_2| < n$. Ou seja, $|r_1 - r_2| = 0$.

Portanto, $r_1 = r_2$ e $a \equiv b \bmod n$.

■

Da proposição anterior temos duas consequências imediatas.

Corolário 2.1 *Sejam a e r inteiros, com $0 \leq r < n$. Então $a \equiv r \bmod n$ se, e somente se, $r = res(a, n)$.*

Demonstração

$\Rrightarrow$ *Seja $a \equiv r \bmod n$. Então $n \mid (a - r)$ e existe* **q** *tal que $(a - r) = nq$. Assim, $a = nq + r$, e, como $0 \leq r < n$, tem-se que $r = res(a, n)$.*

$\Lleftarrow$ *Suponha que $r = res(a, n)$. Então existe um* **q** *tal que $a = nq + r$ e, com isso, $a - r = nq$, o que implica $n \mid (a - r)$. Logo, $a \equiv r \bmod n$.*

■

Corolário 2.2 *Se a e b são inteiros e $a \equiv b \bmod n$, então $n \mid a$ se, e somente se, $n \mid b$.*

Demonstração:

$\Rrightarrow$ *Suponhamos que $a \equiv b \bmod n$. Segue que $n \mid (a - b)$. Como, $n \mid a$ temos que $n \mid b$.*

$\Lleftarrow$ *Se $n \mid a$ e $n \mid b$, temos que $n \mid (a - b)$. Logo, $a \equiv b \bmod n$.*

■

Seja **R** uma relação em um conjunto **A**:

R é Reflexiva se, $\forall a \in A$, aRa.

R é Simétrica se, $\forall a, b \in A$, aRb $\Rightarrow$ bRa.

R é Transitiva se, $\forall a, b, c \in A$, aRb e bRc $\Rightarrow$ aRc.

Uma relação que é Simétrica, Reflexiva e Transitiva é dita uma **Relação de Equivalência**. Assim, temos a seguinte proposição:

Proposição 2.2 *A relação de congruência é uma relação de equivalência.*

Demonstração:

1. ***Reflexiva:*** *$n \mid 0 \Rightarrow n \mid (a-a)$. Pela prop. 2.1, para qualquer* **a** *inteiro, $a \equiv a \, mod \, n$.*

2. ***Sim'etrica:*** *Se $a \equiv b \, mod \, n$, $n \mid (a-b)$. Logo, $n \mid (b-a)$. Desta forma, $b \equiv a \, mod \, n$.*

3. ***Transitiva:*** *Se $a \equiv b \, mod \, n$ e $b \equiv c \, mod \, n$, segue que $n \mid (a-b)$ e $n \mid (b-c)$. Logo, $n \mid ((a-b)+(b-c))$, o que nos dá $n \mid (a-c)$. Portanto, $a \equiv c \, mod \, n$.*

■

Além das propriedades acima citadas, a congruência possui as seguintes propriedades relacionadas às operações, no conjunto dos números inteiros.

Proposição 2.3 *Sejam a,b,c e d inteiros quaisquer. Então:*

1. *Se $a \equiv b \, mod \, n$ e $c \equiv d \, mod \, n$, então $a + c \equiv b + d \, mod \, n$;*

2. *Se $a \equiv b \, mod \, n$ e $c \equiv d \, mod \, n$, então $ac \equiv bd \, mod \, n$;*

3. *Se $m \in \mathbb{Z}_+$ e $a \equiv b \, mod \, n$, então $a^m \equiv b^m \, mod \, n$.*

Demonstração:

1. Se $a \equiv b mod \, n$ e $c \equiv d mod \, n$, segue que $n \mid (a-b)$ e $n \mid (c-d)$. Desta forma, $n \mid ((a-b)+(c-d))$, ou seja, $n \mid ((a+c)-(b+d))$. Portanto, $n \mid (a+c)$ e $n \mid (b+d)$ e $a + b \equiv c + d \, mod \, n$.

2. Se $a \equiv b mod \, n$ e $c \equiv d mod \, n$, segue que $n \mid (a-b)$ e $n \mid (c-d)$. Desta forma, temos $n \mid (d(a-b)+a(c-d))$, que implica em $n \mid (ac-bd)$. Logo, $n \mid bd$ e $n \mid ac$. Então $ac \equiv bd \, mod n$.

3. Sejam $m \in \mathbb{Z}_+$ e $a \equiv b \, mod \, n$. Vamos provar, por indução, que isso é válido $\forall \, m \in \mathbb{Z}_+$.

   Considere P(m) verdadeiro se $a^m \equiv b^m \, mod \, n$.

- Pela hipótese, P(1) é verdade;
- Suponha que P(m) é verdadeiro. Provaremos que P(m+1) também o é.

  $a^m \equiv b^m \, mod \, n$ e $a \equiv b \, mod \, n \Rightarrow a^m a \equiv b^m b \, mod \, n$, pelo item (2) acima.

Isto é, P(m+1) é verdadeiro.

■

Em seguida, relacionaremos congruência às propriedades de divisão.

Proposição 2.4 *Sejam $m, n \in \mathbb{Z}_+$, $m, n > 1$ e $a, b, c \in \mathbb{Z}$:*

1. *Se $a \equiv b \, mod \, \boldsymbol{n}$ e $m \mid n$ então $a \equiv b \, mod \, \boldsymbol{m}$.*
2. *Se $z = mmc(m, n)$ então $a \equiv b \, mod \, n$ e $a \equiv b \, mod \, m$ se, e somente se $a \equiv b \, mod \, z$.*
3. *Se $ac \equiv bc \, mod \, n$ e $mdc(c, n) = 1$, então $a \equiv b \, mod \, n$.*
4. *Se $ab \equiv cd \, mod \, n$, $a \equiv c \, mod \, n$ e $mdc(c, n) = 1$ então $b \equiv d \, mod \, n$.*

Demonstração:

1. Se $a \equiv b \, mod \, n$, $n \mid (a - b)$. Mas, como $m \mid n$, temos que $m \mid (a - b)$. Portanto, $a \equiv b \, mod \, m$.
2. $\Rightarrow$ Se $a \equiv b \, mod \, n$ e $a \equiv b \, mod \, m$, temos que $n \mid (a - b)$ e $m \mid (a - b)$. Desta forma, $mn \mid (a - b)$, ou seja, $z \mid (a - b)$, já que $z = mmc(m, n)$. Logo $a \equiv b \, mod \, z$.
   $\Leftarrow$ Reciprocamente, se $a \equiv b \, mod \, z$, temos $z \mid (a - b)$. Como $z = mmc(m, n)$, $m \mid z$ e $n \mid z$. Portanto, $m \mid (a - b)$ e $n \mid (a - b)$. Logo, $a \equiv b \, mod \, n$ e $a \equiv b \, mod \, m$.

3. Se $ac \equiv bc \, mod \, n$, então $n \mid (ac - bc)$, ou seja, $n \mid c(a - b)$. Mas, $mdc(c, n) = 1$. Então $n \mid (a - b)$. Logo, $a \equiv b \, mod \, n$.

4. Se $ab \equiv cd \, mod \, n$, então $n \mid (ab - cd)$. Se $a \equiv c \, mod \, n$, temos $n \mid (a - c)$. Logo, existem q_1 e q_2 inteiros tais que, $ab - cd = q_1 n$ e $a - c = q_2 n$. Substituindo-se $c = a - q_2 n$, obtemos $ab - ad + dq_2 n = q_1 n$ $\Rightarrow a(b - d) = n(q_1 - dq_2) \Rightarrow n \mid (a(b - d))$. Porém, como $mdc(a, n) = 1$, teremos $n \mid (b - d)$ e $b \equiv d \, mod \, n$.

■

Os itens 3 e 4 são chamados de **Leis do Cancelamento** para congruência, sendo que 4 é a generalização de 3.

Como citado anteriormente, a congruência módulo n é uma relação de equivalência. Desta forma iremos definir uma *classe de equivalência* de a módulo n como:

$$\bar{a} = \{b \in Z \mid a \equiv b \, mod \, n\}$$

Potências Módulo n

Aqui, mostraremos como calcular potências módulo n, para algum $n \in \mathbb{Z}$, com $n > 1$. Ou seja, dados $z, m, n \in \mathbb{Z}$ com $m \geq 0$ e $n > 1$, calcularemos $r = resto(z^m, n)$, ou seja, determinaremos o inteiro r, com $0 \leq r < n$, tal que $z^m \equiv r \, mod \, n$.

Tendo abordado conceitos da Aritmética Modular, podemos continuar nossa exposição sobre a codificação do sistema RSA. Como dito anteriormente, considere $C(b_k)$ o bloco codificado, em que para calcularmos $C(b_k)$ faremos:

$$(b_k)^\sigma \equiv C(b_k) \, mod \, n$$

Seja a seguinte sequência de blocos:

$$142 - 1 - 182 - 8 - 102 - 31 - 61 - 42 - 110$$

Vejamos o que acontece no exemplo que estamos considerando: p = 17, q = 11, n = 187. Ainda precisamos escolher σ. Lembremos que σ será escolhido inversível módulo $\phi(n) = 16.10 = 160$. Escolheremos o menor valor possível para σ que, neste caso, será 3, já que este é o menor número que não divide 160. Assim, o bloco $b_4 = 8$ da mensagem anterior é codificado como o resto da divisão de 8^3 por 187. Observe que $8^3 = 2^9 = 2^8.2$.

Assim, $2^8 = 256 \equiv 69\, mod\, 187$. Então, $8^3 = 2^8.2 \equiv 69.2\, mod\, 187 \Rightarrow 8^3 \equiv 138\, mod\, 187$.

Desta forma a codificação do bloco $b_4 = 8$ é o número 138, ou seja, C(8)=138.

Codificando assim toda a mensagem, temos a seguinte sequência de blocos codificados:

$$131 - 1 - 62 - 138 - 170 - 58 - 150 - 36 - 121$$

Agora, como faremos para decodificar um bloco da mensagem codificada? A informação que precisamos para decodificar consiste em 2 (dois) números: **n** e o inverso multiplicativo de σ com relação a $\phi(n)$, que chamaremos de **d**. O par (n,d) é chamado de **chave de decodificação**. Assim, seja $\mathbf{C(b_k) = a_k}$ um bloco de mensagem codificada. Então $D(a_k)$ será o resultado da decodificação, de tal forma que $D(a_k)$ é o resto da divisão de $(a_k)^d$ por **n**, ou seja,

$$(a_k)^d \equiv D(a_k)\, mod\, n$$

Para obtermos d, basta conhecermos σ e $\phi(n)$ e, assim, aplicar o **Algoritmo de Euclides Estendido**. Primeiramente, definiremos o algoritmo de divisão de Euclides.

Teorema 2.1 ***Algoritmo de Euclides***

Sejam $a, b \in \mathbb{Z}_+, b \neq 0$. *Então existem números inteiros* q *e* r *tais que* $a = bq + r$ *e* $0 \leq r < b$. *Além disso, os valores de* q *e* r *são únicos.*

Demonstração: (Unicidade)

Sejam a e b inteiros positivos e q,q_1 e r,r_1 números inteiros tais que $a = bq + r$ e $a = bq_1 + r_1$ de tal forma que $0 \leq r < b$ e $0 \leq r_1 < b$. Suponha $r_1 \geq r$. Então, se $r = a - bq$ e $r_1 = a - bq_1$, $r - r_1 = (a - bq) - (a - bq_1) \Rightarrow$ $r - r_1 = b(q - q_1)$.

Por outro lado, tanto r quanto r_1 são menores que b. Como supomos $r_1 \geq r$ obtemos $0 \leq r - r_1 < b$. Mas $r - r_1 = b(q - q_1)$, ou seja, $0 \leq b(q - q_1) < 1$. Como q e q_1 são inteiros, $q - q_1 = 0 \Rightarrow q = q_1$. Portanto $r = r_1$.

■

A seguir, alguns teoremas importantes sobre Máximo Divisor Comun de dois inteiros não nulos.

Dizemos que **y** é divisor de **z** (simbolicamente $y \mid z$) se existe **q** tal que $y = zq$ com $y, z, q \in \mathbb{Z}$.

Escrevemos $d = mdc(y, z)$, em que **d** é o máximo divisor comum de y e z. É claro que, se $y \mid z$, $mdc(y, z) = y$. Quando tivermos $mdc(y, z) = 1$, dizemos que y e z são primos entre si. Desta forma, vejamos os seguintes conceitos.

Lema 2.1 *Sejam* y *e* z *dois inteiros positivos. Se* m *e* n *são inteiros tais que* $z = my + n$, *então* $mdc(z, y) = mdc(y, n)$.

Demonstração:

Sejam $d_1 = mdc(z, y)$ e $d_2 = mdc(y, n)$. Temos que $d_1 \mid z$ e $d_1 \mid y$. Logo, existem q_1 e q_2 tais que $z = d_1 q_1$ e $y = d_1 q_2$. Como $d_1 \mid my$ e $d_1 \mid my + n$ temos que $d_1 \mid n$. Deste fato e de que $d_1 \mid y$, temos que d_1 é divisor comum de y e n. Mas, como d_2 é maior divisor comum de y e n, tem–se que $d_1 \leq d_2$.

Partindo-se agora de que $d_2 \mid y$ e $d_2 \mid n$ e que existem q_3 e q_4 tais que $y = d_2q_3$ e $n = d_2q_4$, por substituição tem–se $z = d_2q_3m + d_2q_4$. Então $z = d_2(q_3m + q_4)$, isto é, $d_2 \mid z$. Logo, d_2 é divisor comum entre z e y. Mas, d_1 é o maior divisor comum entre z e y. Desta forma $d_2 \leq d_1$.

Portanto, $d_1 \leq d_2$ e $d_2 \leq d_1$. Assim, $d_2 = d_1$ e $mdc(y, z) = mdc(y, n)$.

■

Observe que o Lema 2.1 nos fornece que:
$mdc(z, y) = mdc(y, z - ym)$ para todo $m \in \mathbb{Z}$.

Exemplo 2.2 *Determine o mdc de 396 e 84; 396 = 4.84 + 60.*

$mdc(396, 84) = mdc(84, 396-84.4) = mdc(84, 60) = mdc(60, 84-60.1) = mdc(60, 24) = mdc(24, 12) = 12$.

Ou seja, $mdc(396, 84) = 12$.

Proposição 2.5 *Sejam a e b inteiros não nulos. Então são válidas as seguintes propriedades:*

1. $mdc(a, b) = mdc(\mid a \mid, \mid b \mid)$.
2. $mdc(a, b) = mdc(b, a)$.

Exemplo 2.3 *Um resultado interessante é o cálculo do* $mdc(n, n^2+1)$, *para* $n \in \mathbb{Z}$ *e* $n > 1$.

$$mdc(n, n^2 + 1) \Rightarrow mdc(n^2 + 1, n)$$
$$\Rightarrow mdc(n, (n^2 + 1) - n.n) \Rightarrow mdc(n, 1)$$
$$\Rightarrow mdc(1, n - n.1) \Rightarrow mdc(1, 0) = 1.$$

Portanto, para qualquer $n \in \mathbb{Z}$, $n > 1$, *temos que* n *e* $n^2 + 1$ *são primos entre si.*

Teorema 2.2 Algoritmo de Euclides Estendido. (Teorema de Bézout) *Dados inteiros positivos não–nulos a e b, tais que* $mdc(a,b) = d$, *com* $d > 0$, *então existem* $m, n \in \mathbb{Z}$ *tais que* $am + bn = d$.

Demonstração:

Seja $M = \{at + bs \mid t, s \in \mathbb{Z}\}$. Então existe algum inteiro não–nulo pertencente a M. Isto é, $M \neq \phi$. Se $x \in M$ então $(-x)$ pertence a M, pois $x = at + bs$ para $t, s \in \mathbb{Z}$, então $(-x) = -(at + bs) = a(-t) + b(-s)$ e $(-t), (-s) \in \mathbb{Z}$.

Seja agora $A = M \bigcap \mathbb{Z}^+$. Pelo Princípio da Boa Ordem, A tem um mínimo, digamos $c = am + bn$. Quero mostrar que $c = d$, em que $d = mdc(a,b)$. Pois bem, $d \mid a$ e $d \mid b$. Então $d \mid am$ e $d \mid bn$ e, logo, $d \mid c$.

Observe que $c \mid a$ e $c \mid b$, pois se $x \in A$ então $x \geq c$ e $x = ta + bs$. Por Euclides, $x = kc + r, 0 \leq r < c$, ou seja, $(ta + bs) = k(am + bn) + r$. Então $(t - km)a + (s - kn)b = r$. E, desta forma, $r = 0$, pois c é mínimo de A. Ou seja, para qualquer $x \in \mathbb{A}$, $c \mid x$. Em particular, $c \mid a$ e $c \mid b$, isto é, $c \mid d$.

Portanto tem–se que $c = d$.

■

Para obtermos então $D(a_k)$, que é o resultado do processo de decodificação, faremos $(a_k)^d \equiv D(a_k)\ mod\ n$. Para encontrarmos **d**, usaremos o Algoritmo de Euclides Estendido. Veja que b_k é o bloco da mensagem original. Então, esperamos que $D(C(b_k)) = b_k$. Em outras palavras, decodificando um bloco da mensagem codificada, esperamos encontrar o bloco da mensagem original.

Insistimos desde o início que codificamos com **n** e decodificamos com **p** e **q**. Porém, vemos que isto não é estritamente verdade, pois além do próprio **n** temos que conhecer o inverso **d** de σ módulo $\phi(n)$. Só conseguimos calcular **d** aplicando o Algoritmo de Euclides Estendido a σ e $\phi(\mathbf{n})$. Assim, no exemplo que estamos acompanhando, $n = 187$ e $\sigma = 3$.

Usando o algoritmo de Euclides para encontrar **d** temos:

$\Phi(187) = 160$. Dividindo-se por 3, temos: $160 = 3.53 + 1$. Ou seja, $1 = 160 + 3.(-53)$.

Desta forma, o inverso multiplicativo de 3 módulo 160 é (-53). Como **d** é expoente, será melhor que d seja inteiro positivo não nulo. Portanto, $d = 160 - 53 = 107$, que é o menor inteiro positivo congruente a (-53) módulo 160. Assim, para decodificarmos o bloco $a_4 = 138$ da mensagem codificada, calculamos $138^{107} \equiv D(a_k) \, mod \, 187$. Calculando via computador, obtemos:

$$138^{107} \equiv 8 \, mod \, 187$$

De tal forma que, $D(a_k) = 8$, ou seja, o bloco original.

2.2.2 Por que funciona?

Como visto acima, o método só é útil se, ao decodificarmos uma mensagem codificada, obtivermos o bloco da mensagem original. Vejamos algumas tentativas, para mostrar que isto realmente acontece.

Seja um sistema RSA com parâmetros **p**, **q** e $\mathbf{n = pq}$. Então as chaves de codificação serão **n** e σ, e os de decodificação serão **n** e **d**. Se b_k é o bloco original, temos que verificar que $D(C(b_k)) = b_k$. Para isto, enunciaremos o seguinte teorema.

Teorema 2.3 *(***Teorema de Euler):** *Sejam $n > 0$ e a números inteiros. Se mdc(a,n) = 1, então,*

$$a^{\phi(n)} \equiv 1 \, mod \, n$$

Veja demonstração em [10] ■

1. **Tentativa I:** Pela definição de **D** e **C** temos.

$$D(C(b_k)) \equiv ((b_k^{\sigma})^d) \equiv (b_k)^{\sigma\, d} \, mod\, n \quad (1)$$

Sabemos que **d** é inverso de σ módulo $\Phi(n)$. Logo, $\sigma\, d = 1 + y\Phi(n)$, para algum $y \in \mathbb{Z}$. Veja que σ e **d** são inteiros maiores que 2, $\Phi(n) > 0$ e $y > 0$. Substituindo em (1), temos:

$$(b_k)^{\sigma\, d} \equiv (b_k)^{1+y\Phi(n)} \equiv b_k(b_k^{\Phi(n)})^y \, mod\, n \quad (2)$$

Se pudermos usar o teorema anterior, teremos, $(b_k)^{\phi(n)} \equiv 1 \, mod\, n$. Desta forma, $(b_k)^{\sigma\, d} \equiv b_k \, mod\, n$. Como queríamos demonstrar.

Porém, só poderemos usar este teorema, se soubermos que o $mdc(b_k, n) = 1$. Isto nem sempre acontece, pois torna-se difícil controlar os valores de b_k, já que estes estão entre 1 e n-1.

A forma para mostrar que o método funciona seria a seguinte.

2. **Tentativa II:** Sabendo que **p** e **q** são primos distintos e $n = pq$, calcularemos a forma reduzida de, $(b_k)^{\sigma\, d}$ módulo **p** e módulo **q**. Assim,

$$\sigma\, d = 1 + y\Phi(n) = 1 + y(p-1)(q-1)$$
$$(b_k)^{\sigma\, d} \equiv b_k(b_k^{p-1})^{y(q-1)} \, mod\, n$$

Se $p \nmid b$ então, usando o **Pequeno Teorema de Fermat**[1], $(b_k)^{p-1} \equiv 1 \, mod\, p$. Logo, $(b_k)^{\sigma\, d} \equiv b_k \, mod\, p$.

Porém nem sempre isso acontecerá, pois não temos como cuidar da escolha dos blocos b_k. Mas, se $p \mid b_k$, $b_k \equiv 0 \, mod\, p$ e a congruência é imediatamente verificada. Assim, $(b_k)^{\sigma\, d} \equiv b_k \, mod\, p$, para todo b_k. Analogamente, podemos mostrar que $(b_k)^{\sigma\, d} \equiv b_k \, mod\, q$.

[1] Cap.3, pág.34

Já que **p** e **q** são primos distintos, teremos $mdc(p, q) = 1$. Pelo Teorema 3.1, temos $pq \mid ((b_k)^{\sigma\, d} - b_k)$. Mas $pq = n$. Assim, $n \mid ((b_k)^{\sigma\, d} - b_k)$ e $(b_k)^{\sigma\, d} \equiv b_k \, mod \, n$, $\forall \, b_k \in \mathbb{Z}$. Portanto, $D(C(b_k)) = b_k$.

■

2.3 Porque o RSA é Seguro

Sejam **p** e **q** primos distintos e $\mathbf{n = pq}$. Sejam (n, σ) a chave de codificação e (n, d) a chave de decodificação. O par (n, σ) é acessível a qualquer usuário, já que se trata da chave pública do sistema.

A segurança do sistema RSA vem da dificuldade em se encontrar **d**, a partir de **n** e σ.

Como vimos, só podemos calcular **d** usando o Algoritmo de Euclides Estendido em σ e $\Phi(n)$. Mas $\Phi(n)$, por outro lado, só pode ser calculado fatorando **n**. Portanto, só podemos quebrar o código se fatorarmos **n**. Se **n** for grande, será difícil realizar esse processo, já que os algoritmos existentes não são rápidos.

Porém, podemos imaginar que haja uma maneira de chegar a **d**, sem fatorar **n**. Por exemplo:

1. **Tentativa I:** Determinar $\Phi(n)$ conhecendo **n**, para encontrar **p** e **q**.

   Conhecendo $\Phi(n)$ e **n**, tem-se que $\Phi(n) = (p-1)(q-1) = pq + 1 - (p+q) = n - (p+q) + 1$, de tal forma que, $(p+q) = n - \Phi(n) + 1$.

   Entretanto $(p+q)^2 - 4n = (p^2 + q^2 + 2pq) - 4pq = (p-q)^2$. Logo, $p - q = \sqrt{(p+q)^2 - 4n}$. Uma vez obtidos $(p+q)$ e $(p-q)$, calculam-se **p** e **q**.

Ao encontrarmos $\Phi(n)$ estaremos fatorando **n**. Se **p** e **q** forem muito pequenos ou muito grandes, mas $\mid p - q \mid$ for pequeno, podemos achar **p** e

q facilmente através do *Algoritmo de Fermat* abaixo, que busca representar $n \in \mathbb{N}$, como a diferença de dois quadrados de números não consecutivos. Lembremos que, se n é ímpar, $n = (\frac{n+1}{2})^2 - (\frac{n-1}{2})^2$.

Algoritmo 2.1 ***(Algoritmo de Fermat)*** *Seja n um número composto e ímpar. Então n é o produto de dois números naturais maiores que 1, calculados do seguinte modo:*

1. *Tome* $\sqrt{n} \leq a < n$*;*
2. *se* $a^2 - n$ *é o quadrado de um natural b, então fatoramos n como (a - b)(a + b);*
3. *se não, incremente a de 1 e volte para 1.*

2.4 Assinatura Digital

É o modo pelo qual dois meios de comunicação obtêm segurança no recebimento e envio de uma mensagem. Para que isso ocorra são emitidos certificado e credenciais, em que: certificado é o documento de garantia, válido por tempo determinado; credencial é o poder outorgado a uma pessoa ou a uma entidade.

A assinatura digital existe para que, em uma transação entre dois meios de comunicação, haja credibilidade no que está sendo transmitido. Para isso, seguem-se os seguintes princípios:

1. **Autenticação:** Identificação da pessoa ou entidade;
2. **Confiabilidade:** Privacidade da informação;
3. **Integridade:** A informação não é modificada durante a transação;
4. **Não Repúdio:** A origem não pode negar a autoria.

Nos documentos de papel, a segurança vem através do timbre, assinatura original e documento original, bem como a confiabilidade com os envelopes lacrados.

Já no documento digital, a segurança surge justamente através da autenticação, integridade e o não repúdio, bem como da confiabilidade da criptografia.

A criptografia RSA opera com duas chaves relacionadas: uma pública e outra privada. A chave pública é divulgada e a chave privada é gerada e mantida no ambiente operacional.

2.4.1 Como Funciona?

Sejam C_a e D_a as funções codificação e decodificação do local **A**; e C_b e D_b as funções correspondentes ao local **B**.

Se A quer enviar um bloco **a** de uma mensagem, deveriamos enviar $C_b(a)$, mas, para manter a mensagem assinada, enviamos $C_b(D_a(a))$. Quando B recebe, primeiro ela aplica D_b para obter $D_a(a)$, e a este aplica $C_a(a)$. Note que $C_a(a)$ é conhecido, pois é pública.

Desta forma B tem segurança de que recebeu uma mensagem verdadeira, pois ao usar funções D_bC_a nota–se que a mensagem faz sentido, mesmo porque D_a só é conhecido pelo local A.

Capítulo 3

Teste de Primalidade

Em um sistema de cifragem assimétrico é importante escolher de modo eficiente os parâmetros das chave pública e privada. No sistema de cifragem RSA, geramos dois inteiros primos p e q para obter o módulo n = pq. Neste caso, os primos p e q devem ser "grandes"o suficiente para que a fatoração de n seja extremamente difícil. Os primos devem ser "aleatórios"no sentido em que a probabilidade de escolher um primo em particular é suficientemente pequena. Neste capítulo, veremos alguns métodos que consistem em gerar, aleatóriamente números de um determinado tamanho e verificar se este é primo, mesmo que lentos e difíceis de se usar.

Inicialmente, vejamos algumas propriedades dos números primos.

3.1 Propriedades Fundamentais dos Primos

Lema 3.1 *Sejam* $a, b, c \in \mathbb{Z}^+$ *e suponhamos que* $mdc(a, b) = 1$.

1. $b \mid ac \Rightarrow b \mid c$.

2. $a \mid c \ \ e \ \ b \mid c \Rightarrow ab \mid c$.

Demonstração:

1. Pela hipótese, tem-se que $mdc(a, b) = 1$. Pelo Algoritmo de Euclides Estendido, existem $m, n \in \mathbb{Z}^*$ tais que $ma + nb = 1$ (1)

   Multiplicando ambos os lados de (1) por c, temos $mac + nbc = c$. Veja que $b \mid nbc$ e $b \mid mac$, pela hipótese do item 1. Portanto, mac + nbc é divisível por b e, consequêntemente, $b \mid c$.

2. Temos que se $a \mid c$, então $c = aq$, para todo $q \in \mathbb{Z}$. Mas b também divide c. Como $mdc(a, b) = 1$, então $b \mid t$, com $t = bp$ para todo $p \in \mathbb{Z}$. Desta forma, $c = at = (ab)p$. Portanto c é divisível por ab.

■

Teorema 3.1 ***(Propriedade Fundamental dos Primos):***

Sejam p um número primo e $a, b \in \mathbb{Z}^+$. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração:

Suponha que p não divide a. Então, como p é primo, temos que p e a são primos entre si. Por hipótese, $p \mid ab$. Assim, pelo lema 3.1, $p \mid b$.

■

Teorema 3.2 (Teorema Fundamental da Aritmética) *Todo número inteiro positivo n, $n \neq 1$, pode ser escrito de forma única como um produto de primos, ou seja,*

$$n = p_1.p_2.....p_t.$$

onde $p_1 \leq p_2 \leq \ldots \leq p_t$ são números primos.

Ver demonstração em [3]

■

Teorema 3.3 *Em $\mathbb{Z}$ existem infinitos números primos.*

Demonstração: Suponha que o conjunto dos números primos é finito. Seja p o maior primo positivo deste conjunto e considere **a** formado de todos os primos positivos deste conjunto menos 1:

$$a = (2.3.5.7.\cdots.p) - 1$$

Como $a \neq 0$ e $a \neq \pm 1$, pelo teorema 2.3, temos que **a** tem um divisor primo **q** positivo. Como **q** é primo, ele é um dos fatores $(2.3.5.\cdots.p)$. Logo, temos que $q \mid (-1)$, o que é absurdo.

■

Lema 3.2 *Seja $a > 0$. Se $n = pq$, q um número ímpar, então $(a^p + 1) \mid (a^n + 1)$.*

Demonstração:

Temos que $a^p \equiv (-1)\, mod\, (a^p + 1) \Rightarrow a^{pq} \equiv (-1)^q\, mod\, (a^{pq} + 1) \Rightarrow$
$a^n \equiv (-1)\, mod\, (a^p + 1) \Rightarrow (a^n + 1)$ *é múltiplo de* $(a^p + 1)$

■

Lema 3.3 *Seja $a > 0$. Se $n = pq$, q um número ímpar, então $(a^p - 1) \mid (a^n - 1)$.*

Demonstração:

Temos que $a^p \equiv 1\, mod\, (a^p - 1) \Rightarrow a^{pq} \equiv 1^q\, mod\, (a^{pq} - 1) \Rightarrow$
$a^n \equiv 1\, mod\, (a^p - 1) \Rightarrow (a^n - 1)$ *é múltiplo de* $(a^p - 1)$

■

3.2 Determinando Números Primos

Como dito anteriormente, queremos encontrar algoritmos que nos ajudem a decidir se um número é primo ou não.

Uma das formas mais antigas de se listar números primos é através do Crivo de Eratóstenes *e, para isso, usaremos o seguinte resultado.*

3.2.1 Crivo de Eratóstenes

Lema 3.4 *Se $n \in \mathbb{Z}$, $n > 1$, não é divisível por nenhum primo positivo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração: *Suponhamos que n não seja primo e p é o menor primo positivo que divide n. Desta forma:*

$$n = pm \ com \ p \leq m$$

assim, $p^2 \leq pm = n$. Desta forma, n é divisível por p primo talque $p^2 \leq n$. Absurdo.

■

Vejamos como seria o Crivo de Eratóstenes até 150.

1	$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9	10
$\boxed{11}$	12	$\boxed{13}$	14	15	16	$\boxed{17}$	18	$\boxed{19}$	20
21	22	$\boxed{23}$	24	25	26	27	28	$\boxed{29}$	30
$\boxed{31}$	32	33	34	35	36	$\boxed{37}$	38	39	40
$\boxed{41}$	42	$\boxed{43}$	44	45	46	$\boxed{47}$	48	49	50
51	52	$\boxed{53}$	54	55	56	57	58	$\boxed{59}$	60
$\boxed{61}$	62	63	64	65	66	$\boxed{67}$	68	69	70
$\boxed{71}$	72	$\boxed{73}$	74	75	76	77	78	$\boxed{79}$	80
81	82	$\boxed{83}$	84	85	86	87	88	$\boxed{89}$	90
91	92	93	94	95	96	97	98	99	100
$\boxed{101}$	102	$\boxed{103}$	104	105	106	$\boxed{107}$	108	$\boxed{109}$	110
$\boxed{111}$	112	$\boxed{113}$	114	115	116	117	118	$\boxed{119}$	120
121	122	123	124	125	126	127	128	129	130
$\boxed{131}$	132	$\boxed{133}$	134	135	136	$\boxed{137}$	138	$\boxed{139}$	140
$\boxed{141}$	142	$\boxed{143}$	144	145	146	147	148	149	150

Tabela 3.1: Números primos menores que 150

3.2.2 Teste de Mersenne

Proposição 3.1 *: Sejam $a, n \in \mathbb{Z}$ e $a, n > 1$. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.*

Demonstração: *Suponha que $a^n - 1$ é primo. Tem–se que $a \neq 1$. Então, como $(a-1) \mid (a^n - 1)$, $a - 1 = \pm 1$. Daí segue que a única possibilidade é $a = 2$. Suponha agora, por absurdo, que n não é primo. Assim, $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Segue, pelo lema 3.3, que $2^n - 1$ não é primo.*

■

Definição 3.1 *Para todo $n > 1$ inteiro, $M(n) = 2^n - 1$ é o n–ésimo número de Mersenne.*

3.2.3 Testes de Fermat

Veremos a seguir alguns conceitos que nos ajudarão a entender os testes para primalidade de Fermat.

Proposição 3.2 *Sejam $n, p \in \mathbb{Z}$ com $1 < p < n$, então:*

1. *$p!$ divide $n(n-1)(n-2).\cdots.(n-p+1)$.*

2. *$p!.(n-p)!$ divide $n!$.*

Veja demonstração em [3]

Definição 3.2 *Um Número Binomial n sobre p é:*

$$\left(\begin{array}{c} n \\ p \end{array} \right) = \left(\begin{array}{c} \dfrac{n!}{p!(n-p)!},\ se\ \ n \geq\ p \\ 0, \quad se\ \ n < p \end{array} \right)$$

Lema 3.5 *Se p é um número primo e $n \in \mathbb{Z}$ tal que $1 \leq\ n < p$, então p é divisor de $\left(\begin{array}{c} p \\ n \end{array} \right)$.*

Demonstração: *Pelas definições 2.1 e 2.2 tem–se que:*

$$n!(p-n)!.\left(\begin{array}{c} p \\ n \end{array} \right) = p!$$

que mostra que p divide o produto $n!(p-n)!.\left(\begin{array}{c} p \\ n \end{array} \right)$. Pela Propriedade dos números primos, $p \mid n!$ ou $p \mid (p-n)!$ ou $p \mid \left(\begin{array}{c} p \\ n \end{array} \right)$. Se $p \mid n!$ ou $p \mid (p-n)!$, pela mesma propriedade, $p \mid 1$ ou $p \mid 2$ ou $\cdots$ $p \mid n$ ou $\cdots$ $p \mid (p-1)$. Mas $1, 2, \cdots, n, p-1$ são menores que p.

Portanto $p \mid \left(\begin{array}{c} p \\ n \end{array} \right)$.

■

Teorema 3.4 **(Pequeno Teorema de Fermat):** *Para qualquer $a \in \mathbb{Z}$, se $p > 0$ é primo, então $p \mid (a^p - a)$, ou seja, $a^p \equiv a \, mod \, p$.*

Demonstração: *Analisaremos os seguintes casos:*

1. *$p = 2$.*
2. *p é primo e $p \neq 2$.*

- *Caso 1. Se $p = 2$, então $a^2 - a$ é um número par, pois $a^2 - a = a(a-1)$, ou seja, o produto de dois números consecutivos.*
- *Caso 2. $p \neq 2$.*

  Se $a < 0$ então, $-(a^p - a) = \mid a^p \mid - \mid a \mid$. Ou seja, basta considera $a > 0$. Vamos fazer uma indução sobre a. Seja p primo e seja $P(a)$ a proposição $p \mid (a^p - a)$.

  Desta forma, P(1) é verdadeiro pois $1^p - 1 = 0$ e $p \mid 0$. Suponhamos que $P(a)$ é verdadeiro e vamos provar que $P(a+1)$ também o é..

  Usando a fórmula do Binômio de Newton, temos que:

$$(a+p)^p - (a+1) = a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + \begin{pmatrix} p \\ 2 \end{pmatrix} a^{p-2} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a +$$

$$1 - a - 1 = (a^p - a) + pa^{p-1} + \begin{pmatrix} p \\ 2 \end{pmatrix} a^{p-2} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a$$

  Pela hipótese de indução $p \mid (a^p - a)$. Pelos lemas anteriores, p divide as demais parcelas. Portanto, $p \mid ((a+1)^p - (a+1))$.

■

Exemplo 3.1 *Seja $p = 3007$ e $a = 2$. Será que p é primo ? Veja que*

$$2^{3007} \equiv 33 \, mod \, 3007$$

Se 3007 fosse primo teríamos $2^{3007} \equiv 2 \, mod \, 3007$. *Desta forma 3007 não é primo.*

Teorema 3.5 *Sejam a e p inteiros positivos. Se* $a^p \not\equiv a \, mod \, p$, *então p não é primo.*

Teorema 3.6 Pequeno Teorema de Fermat II: *Sejam p um número primo e a um inteiro que não é divisível por p. Então* $a^{p-1} \equiv 1 \, mod \, p$.

Proposição 3.3 *Sejam* $a, n \in \mathbb{Z}$ *e* $a, n > 1$. *Se* $a^n + 1$ *é primo, então a é par e* $n = 2^m$ *com* $m \in \mathbb{Z}^+$.

Demonstração: *Suponha que* $a^n + 1$ *é primo.*

Segue que a tem que ser par, pois do contrário temos $2 \mid a^n+1$ *e* $a^n+1 > 2$, *que é absurdo. Seja agora* $n = 2^m r$, *com* $m \in \mathbb{Z}^+$, $r \in \mathbb{N}$ *e* $2 \nmid r$. *Vamos mostrar que* $r = 1$. *Sendo r ímpar, segue pelo lema 3.2 que* $a^{2^m} + 1 \mid a^n + 1 = (a^{2^m})^r + 1$. *Como supomos que* $a^n + 1$ *é primo, isto só pode acontecer se* $a^{2^m} + 1 = a^n + 1$. *Portanto* $r = 1$.

■

Definição 3.3 (Números de Fermat): $F_n = 2^{2n} + 1$, *em que* $n \geq 1$, *é chamado de n–ésimo número de Fermat.*

A proposição seguinte é um critério no qual decide-se se um número desta forma é primo.

Proposição 3.4 (Pepin): $F_n = 2^{2n} + 1$, *para algum* $n \geq 1$, *é primo se e somente se* $3^{2^{2^n-1}} \equiv -1 \, mod \, F_n$.

Veja a demonstração em [2].

Definição 3.4 *Sejam* $n \geq 3$ *um inteiro ímpar e* $1 \leq b < n$, *inteiro. Dizemos que n é pseudoprimo na base b se* $b^{n-1} \equiv 1 \, mod \, n$.

Definição 3.5 *Seja n um número inteiro ímpar composto e seja* a *tal que* $1 < a \leq n-1$. *Diz-se que* n *é um* pseudoprimo *de Fermat para a base* ***a*** *se* $a^{n-1} \equiv 1 \, mod \, n$.

3.3 Teste para Pseudoprimos

3.3.1 Teste de Carmichael

Lembremo-nos de que se n é um número composto, então existe um natural menor ou igual a $\sqrt{n}$ *que divide n.*

Algoritmo 3.1 *Seja* $n \in N$. *Se n for divisível por algum natural entre 2 e* $\sqrt{n}$, *então n é composto. Caso contrário n é primo.*

Algoritmo 3.2 *Sejam* $k, n \in N$. *Escolhemos randomicamente elementos* $a_1, a_2, \ldots, a_k$ *entre 1 e n - 1. Se* $mdc(a_k, n) = 1$ *e se* $a_i^{n-1} \equiv 1 \, mod \, n$, *para todo* $i \in 1, \cdots, k$. *Então, n é primo. Caso contrário, n é composto.*

Este último algoritmo nem sempre é válido, pois não mostramos que existe $a_i \in Z_n^*$, *tal que* $a_i^{n-1} \not\equiv 1 mod n$. *Pois, se n for composto, existe a possibilidade de que n, mesmo assim, passe no teste.*

Definição 3.6 *Seja n um número inteiro composto. Diz-se que n é um número de* Carmichael *se* $a^{n-1} \equiv 1 \, mod n$, $\forall \, a \in Z_n$, *tal que mdc(a, n) = 1, isto é, em outras palavras, se n é um pseudoprimo para todas as bases a que são primas com n.*

Teorema 3.7 *Um inteiro positivo n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as duas condições:*

1. $p^2 \nmid n$
2. $p - 1 \mid n - 1$

3.3.2 Teste de Miller

Há um teste que detecta números compostos com muita eficiência. Este teste é conhecido como O teste de Miller.

Algoritmo 3.3 (Teste de Miller): *Seja $n \geq 3$ um número ímpar e b um inteiro tal que $1 \leq b < n$, em que mdc(b,n) = 1. Se n for primo,*

1. $b^{2^k q} \equiv 1 \, mod \, n$, *com* $k, q \in \mathbb{Z}$;
2. $b^q \equiv 1 \, mod \, n$;
3. *existe* $1 \leq j \leq k-1$ *tal que* $b^{j-1} \equiv -1 \, mod \, n$.

Definição 3.7 *Seja $n \geq 3$ ímpar e composto tal que n satisfaça o Teste de Miller para algum $1 \leq b < n$, com mdc(b,n)=1. Nesta condições dizemos que n é pseudoprimo forte na base b.*

3.3.3 Teste de Rabin

De posse da proposição a seguir, modificaremos o Algoritimo 3.2, obtendo assim o algoritmo probabilístico de Rabin.

Proposição 3.5 *Seja $n > 1$, n composto, ímpar. Então o número de inteiros a, $0 < a < n$, para os quais n é um pseudoprimo na base a é menor do que $\frac{n}{4}$.*

Algoritmo 3.4 *Sejam $k, n \in N$, com n ímpar. Escolha randomicamente $a_1, a_2, \ldots, a_k$, entre 1 e n - 1. Se $mdc(a_i, n) = 1$ e n for pseudoprimo com relação a base a_i, para todo $i \in \mathbb{Z}$, então n é primo.*

3.3.4 Teste de Miller-Rabin-HRE

Definição 3.8 *Seja n um inteiro positivo. Um carácter módulo n é uma função* $\chi : \mathbb{Z}_n^* \longrightarrow \mathbb{C}$ *, tal que.*

1. $\chi(k) = 0$, *quando* $mdc(k, n) \neq 1$;
2. $\chi(k) = \chi(l)$ *quando* $k \equiv l \bmod n$;
3. $\chi(kl) = \chi(k)\chi(l)$;
4. $\chi(1) \neq 0$.

Definimos ainda o carácter principal módulo n como sendo:

$$\chi_1(m) = \begin{pmatrix} 1, & se \quad mdc(m,n) = 1 \\ 0, & se \quad mdc(m,n) \neq 1 \end{pmatrix}$$

Para todo o carácter χ*, a L–função de* Dirichlet *para* χ *é definida pela seguinte série infinita:*

$$L(s, \chi) = \sum_{k=0}^{\infty} \frac{\chi(k)}{k^s}$$

Conjectura 3.1 (Hipótese de Riemann Estendida) *Para todo carácter* χ*, os zeros da função* L_χ *em* $\{z \in \mathbb{C} : 0 < Re(z) \leq 1\}$ *estão sobre a reta* $Re(z) = \frac{1}{2}$.

Teorema 3.8 (Bach) *Seja G um subconjunto de* $\mathbb{Z}_n^*$ *fechado com relação a multiplicação. Se* $G \neq \mathbb{Z}_n^*$*, então existe* $a \in \mathbb{Z}_n^* \setminus G$ *tal que* $a < 2\log^2 n$.

Teorema 3.9 *Se n for composto e ímpar, então existe* $1 \leq a < 2\log^2 n$ *tal que n é um pseudoprimo com relação à base a.*

Veja demonstração em [8].

Com estes resultados e assumindo como verdadeira a Hipótese de Riemann Estendida.

Algoritmo 3.5 (Miller-Rabin-HRE) *Seja n um inteiro ímpar. Se n é pseudoprimo para todas bases $a < 2\log^2(n)$ e a Hipótese de Riemann Estendida for verdadeira, então n é primo. Caso contrário n é composto.*

3.4 Teste para Primos

Na seção de Pseudoprimos obtivemos testes de primalidade do tipo: os números que não passam no teste são compostos. Desta vez obteremos testes que dizem que os números que passam no teste são primos. Para que possamos prosseguir precisaremos da seguinte definição.

Definição 3.9 *Seja G um grupo com elemento neutro 1. Seja $x \in G$. Se $\{n \geq 1 \mid x^n = 1\} \neq \emptyset$, então definimos $o(x) = min\{n \geq 1 \mid x^n = 1\}$. Caso contrário, $o(x) = 1$. Esse número $o(x)$ é dito a ordem de x.*

Assim, vejamos o seguinte teste.

3.4.1 Teste de Lucas

Teorema 3.10 (Teste de Lucas): *Seja $n \geq 3$ inteiro. Suponha que exista $1 \leq b \leq n-1$ inteiro, tal que para todo fator primo de n-1, tenhamos $b^{n-1} \equiv 1 \, mod \, n$ e $b^{(n-1)b} \not\equiv 1 \, mod \, n$. Então n é primo.*

Demonstração: *Seja $d = o(\bar{b})$ em $\mathbb{Z}_n$. Como $\bar{b}^{(n-1)} = 1$, temos que $d \mid (n-1)$, digamos n - 1 = kd, para $k \geq 1$ inteiro. Assim basta mostrar que k = 1. Suponhamos que $k > 1$. Seja p um fator primo de k. Logo, p*

também é um fator primo de n-1. Note que $\frac{n-1}{p} = \frac{k}{p}d$ *e que* $\frac{n-1}{p}, \frac{k}{p} \in \mathbb{Z}$. *Logo,* $\overline{b}^{(\frac{n-1}{p})} = (\overline{b}^{d})^{\frac{k}{p}} = 1$, *o que contradiz a hipótese do teorema.*

■

Teorema 3.11 (Teste de Lucas Generalizado): *Seja* $n \geq 3$ *inteiro e seja* $n-1 = p_1^{e_1} \cdots p_r^{e_r}$ *a fatoração de n-1. Suponha que para cada* $1 \leq i \leq r$ *existe* $1 \leq b \leq n-1$ *inteiro, tal que* $(b_i)^{n-1} \equiv 1 \, mod \, n$ *e* $b_i^{\frac{(n-1)}{p_i}} \not\equiv 1 \, mod \, n$. *Então n é primo.*

Demonstração: *Seja* $d_1 = o(b_1)$. *Então* $d_1|(n-1)$, *pois* $\overline{b}_1^{n-1} = \overline{1}$. *Neste caso,* $d_1 = p_1^{f_1} \cdots p_r^{fr}$, *em que* $0 \leq f_i \leq e_i$ *são inteiros não negativos. Por outro lado,* $\overline{b}_1^{n-1} \neq \overline{1}$, *i.e.,* $d \nmid \frac{n-1}{p_1} = p_1^{e_1} \cdots p_r^{e_r}$. *Mas a única possibilidade para isto ocorrer é que* $f_1 = e_1$. *Portanto,* $p_1^{e_1}|d$. *Repetindo o mesmo argumento para os outros elementos* b_i, *concluimos que, para todo* $1 \leq i \leq r, p_i^{ei} \mid d$. *Assim,* $n-1 = p_1^{e1} \cdots p_r^{er} \mid d$, *i.e.,* $n-1 \leq d \leq \phi(n) \leq n-1$. *Logo,* $n-1 = \phi(n)$ *e n é primo.*

■

Existem diversos outros testes determinísticos de números primos: ***Teste de Alenstra, Teste de Gauss, Teste de Miller–Rabin, Algoritmo AKS, Teste de Monte Carlo,Teste de Solovay–Strassen****. Estes testes podem ser encontrados, por exemplo, em [8].*

Capítulo 4

Uma Aplicação do Sistema RSA

4.1 Definindo Parâmetros

Neste capítulo, definirei meus próprios parâmetros pois, como afirmei no início deste trabalho, a escolha dos valores associados aos caracteres que iremos utilizar é aleatória. Desta forma, usarei letras maiúsculas e minúsculas, acentos, pontuações e algarismos, os quais terão os seguintes valores associados:

1. *Letras do Alfabeto Maiúsculas:*

$$\begin{array}{lllllll} A \to 120 & B \to 121 & C \to 122 & D \to 123 & E \to 124 & F \to 125 & G \to 126 \\ H \to 127 & I \to 128 & J \to 129 & K \to 130 & L \to 131 & M \to 132 & N \to 133 \\ O \to 134 & P \to 135 & Q \to 136 & R \to 137 & S \to 138 & T \to 139 & U \to 140 \\ V \to 141 & W \to 142 & X \to 143 & Y \to 144 & Z \to 145 & & \end{array}$$

2. *Letras do Alfabeto Minúsculas:*

$a \to 146$ $b \to 147$ $c \to 148$ $d \to 149$ $e \to 150$ $f \to 151$ $g \to 152$
$h \to 153$ $i \to 154$ $j \to 155$ $k \to 156$ $l \to 157$ $m \to 158$ $n \to 159$
$o \to 160$ $p \to 161$ $q \to 162$ $r \to 163$ $s \to 164$ $t \to 165$ $u \to 166$
$v \to 167$ $w \to 168$ $x \to 169$ $y \to 170$ $z \to 171$

3. Algarismos:

$0 \to 172$ $1 \to 173$ $2 \to 174$ $3 \to 175$ $4 \to 176$ $5 \to 177$ $6 \to 178$
$7 \to 179$ $8 \to 180$ $9 \to 181$

4. Acentos e Pontuações:

$. \to 182$ $, \to 183$ $: \to 184$ $á \to 185$ $é \to 186$ $í \to 187$ $ó \to 188$
$ú \to 189$ $â \to 190$ $ã \to 191$ $ô \to 192$ $õ \to 193$ $ê \to 194$ $- \to 195$

5. O Espaço entre as palavras será dado por 99.

Os valores associados foram escolhidos desta forma porque os parâmetros que escolherei serão dois primos de pelo menos 4 algarismos. Desta forma, ao determinarmos n, como sendo o produto dos primos, teremos um número grande, o qual nos possibilitará dividir a mensagem escolhida em blocos com uma quantidade maior de algarismos, tornando assim mais difícil a decodificação.

Sejam $p = 1013$ *e* $q = 9941$, *p e q primos. Desta forma seja n o produto de p por q. Assim,* $n = 10070233$. *Podemos passar à etapa de Pré–codificação.*

4.1.1 Pré Codificação

Neste momento escolho a mensagem a ser enviada, para que possa ser feita a conversão. Desta forma, converterei a seguinte mensagem:

A dúvida é um dos nomes da Inteligência – Jorge Luis Borges –

Codificando a mensagem acima, teremos um número, que é formado pela substituição das letras por seu valores associados (etapa anterior).

A dúvida é um dos nomes da Inteligência – Jorge Luis Borges –
1209914918916715414912099186166158991491601639915916015 8
150164991491469912815816515015715415219415914815414 6

Tendo feito a conversão, vamos quebrar esta sequência de números em blocos b_k, com $k > 1$, de tal forma que seu valor numérico seja menor que n=10070233. Portanto, consideremos os seguintes blocos:

1209914–9189167–1541491–2099186–1661589–9149160–1639915–
9160158–1501649–9149146–99128–1581651–5015715–4152194–
159148–154146

Terminada esta etapa, partiremos para a Codificação RSA da mensagem.

4.2 Codificação

Nesta etapa, precisamos da chave de codificação, que é formada pelo par (n, σ), de tal forma que σ seja um inteiro inversível módulo $\phi(n)$, em que $\phi(n) = (p-1)(q-1) = 10059280$. Escolherei σ como sendo o menor número cujo $mdc(\phi(n), \sigma) = 1$. Desta forma, obtemos $\sigma = 3$. Convertendo o bloco $b_1 = 1209914$, teremos:

$$b_1^3 \equiv C(b_1) \, mod \, n$$

ou seja,

$$(1209914)^3 \equiv C(1209914) \, mod \, 10070233$$
$$(1209914)^3 \equiv 2504405 \, mod \, 10070233$$

Desta forma, $C(b_1) = C(1209914) = 2504405$.[1]

Fazendo o mesmo para todos os blocos b_k*, tais que* $k, n \in \mathbb{Z}_+$*, temos as seguintes conversões:*

(b_k), k=2n+1	$C(b_k)$	(b_k), k=2n + 2	$C(b_k)$
1209914	***2504405***	*9189167*	***8166157***
1541491	***044486***	*2099186*	***6484701***
1661589	***286993***	*9149160*	***6505576***
99128	***6731185***	*1581651*	***57631***
5015715	***10050479***	*4152194*	***5004185***
159148	***798570***	*154146*	***6050599***

resultando, assim, na mensagem codificada.

2504405–8166157–7044486–6484701–286993–6505576–
905164–7812557–6731185–57631–10050479–5004185–
798570–6050599

4.3 Decodificação

Tendo feito o processo de codificação, passaremos a etapa na qual o destinatário irá ler a mensagem codificada.

Portanto, considere a seguinte mensagem codificada.

2504405–8166157–7044486–6484701–286993–6505576–
905164–7812557–6731185–57631–10050479–5004185–
798570–6050599

Para decodificarmos, precisamos da chave privada, que consiste em dois números (n,d), de tal forma que **n** *é o produto de dois primos (os mesmos*

[1] O cálculo foi realizado pelo algoritmo restopot.m, Apêndice A

usados para codificar), e **d** *seja inverso de* σ *com relação a* $\phi(n)$*. Portanto, usando o algoritmo de Euclides Estendido para encontrar d, temos:*

$$\phi(n) = \sigma.q + 1$$

$$1 = \phi(n) + \sigma(-q)$$

Assim, o inverso de σ *módulo* $\phi(n)$ *é (-q). Como d é expoente, é melhor tê-lo positivo. Assim, faremos*

$$d = \phi(n) + (-q)$$

Portanto, teremos:

$$10059280 = 3.3353093 + 1$$

$$1 = 10059280 + 3(-3353093)$$

$$d = 10059280 + (-3353093) \Rightarrow d = 6706187$$

Contudo, vamos denotar $C(b_k) = c_k$*, um bloco da mensagem codificada. Para decodificarmos um bloco* c_k*, usaremos a seguinte fórmula:*

$$(c_k)^d \equiv\ D(c_k)\, mod\, n$$

de tal forma que $D(c_k) = b_k$*, ou seja, a decodificação de um bloco* c_k *resulte em seu bloco original* b_k*.*

Então, para o bloco $c_1 = 2504405$*, obtemos o seguinte resultado:*

$$(c_1)^d \equiv\ D(c_1)\, mod\, n$$

$$(2504405)^{6706187} \equiv\ D(c_1)\, mod\, 10070233$$

$$(2504405)^{6706187} \equiv\ 1209914\, mod\, 10070233$$

Ou seja, $D(c_1) = 1209914 = b_1$ [2]

Realizando o mesmo processo, para todos o blocos c_k*, tal que* $k, n \in \mathbb{Z}_+$*, teremos:*

(c_k), k=2n+1	$D(c_k)$	(c_k), k=2n + 2	$D(c_k)$
2504405	*1209914*	***8166157***	*9189167*
044486	*1541491*	***6484701***	*2099186*
286993	*1661589*	***6505576***	*9149160*
6731185	*99128*	***57631***	*1581651*
10050479	*5015715*	***5004185***	*4152194*
798570	*159148*	***6050599***	*154146*

resultando, assim, na mensagem original.

1209914–9189167–1541491–2099186–1661589–9149160–1639915–
9160158–1501649–9149146–99128–1581651–5015715–4152194–
159148–154146

Resta, neste momento, substituir os valores da mensagem por suas respectivas letras, formando a mensagem.

A dúvida é um dos nomes da Inteligência – Jorge Luis Borges –

O método funciona claramente para a pessoa que envia e para a que recebe. Basta as mesmas possuirem as chaves pública e privada, de tal forma que somente a pessoa que recebe tenha a chave privada.

[2] O cálculo foi realizado pelo algoritmo restopot.m, Apêndice A

Conclusão

Através do presente trabalho, a criptografia se mostra essencial na evolução humana. A busca pela segurança cresce, juntamente com a necessidade em sentir confiança na transmissão de informações que nos é feita. Desta forma, desenvolveram-se diversos métodos, dentre eles o RSA, baseado nos números primos.

Conceitos básicos, como Máximo Divisor Comum e Algoritmo de Divisão, mostram sua contribuição em nosso dia–a–dia, de tal forma que a matemática confirma sua importância na vida prática.

Houve muitos desafios, em especial, na implementação da aplicação do método RSA, que só aumentaram minha curiosidade e vontade em continuar a aprender. Desta forma, creio que este trabalho atingiu os objetivos propostos.

Apêndice A

Algoritmo de Codificação e Decodificação

Para codificarmos e decodificarmos os blocos b_k *e* c_k*, respectivamente, usamos o seguindo algoritmo, que calcula* r*,* $0 \leq r < p$*, tal que* $n^q \equiv r \, mod \, p$*.*

function r = restopot(n,q,p)

%RESTOPOT, resto da divisão da potência de um número por outro número.

%r=restopot(n,q,p) calcula o resto da divisão de n^q *por p.*

%Licio H. Bezerra

%Copyright. 2005. Matemática/UFSC

a = dec2bin(q);

m = length(a);

b = a(m:-1:1);

x = mod(n,p);

i=1;

```
zero = dec2bin(0);
while b(i) == zero
x = mod(x^2,p);
i = i + 1;
end r = mod(x,p);
for j = i + 1:m
x = mod(x^2,p);
if ~(b(j) == zero), r = mod(r*x,p); end
end
```

Referências Bibliográficas

[1] Abramo Hefez - Curso de Álgebra - Rio de Janeiro: SBM, 1993.

[2] Adilson, Gonçalves - Introdução à Álgebra - Rio de Janeiro: SBM, 1977.

[3] Amilcar Pacheco - Álgebra - Notas de Aula, Universidade Federal do Rio de Janeiro, Rio de Janeiro: 2002.

[4] Arnaldo Garcia & Yves, Lequain - Álgebra: um curso de introdução - Rio de Janeiro: SBM, 1988.

[5] E. R. Sheinerman - Matemática Discreta - Uma Introdução - São Paulo: Thomson Learning, 2003.

[6] Jacy L. H. Monteiro - Elementos de Álgebra - Rio de Janeiro: Ao Livro Técnico S.A., 1969.

[7] Jaime, Evaristo & Eduardo, Perdigão - Introdução a Álgebra Abstrata, Maceió: EDUFAL, 2002.

[8] Jorge M.L. Santos - O uso de cifragem para proteção de canais abertos - Dissertação de Mestrado, Faculdade de Ciências da Universidade do Porto: 2002.

[9] Manuel Lemos - Criptografia, Números Primos e Algoritmos - 17 Colóquio Brasileiro de Matemática, Rio de Janeiro: SBM, 2001.

[10] S. C. Coutinho - Números Inteiros e Criptografia RSA - Série de Computação e Matemática, Rio de Janeiro: SBM, 1997.

[11] Viktoria Tkotz - Criptografia - Segredos Embalados para Viagem - disponível em http://www.numaboa.com.br/criptologia /criptografia.php: acesso em 03/06/2005.